КРИТОГРАФИЯ. КЛАССИЧЕСКИЕ И СОВРЕМЕННЫЕ ШИФРЫ

Криптография – это наука о методах шифрования и дешифрования информации, которая описывает алгоритмы, методы и математические модели, используемые для защиты данных от несанкционированного доступа, изменения или уничтожения. Криптографические методы используются в различных сферах, включая защиту электронной почты, банковских операций, конфиденциальных документов и т.д.

Существует два основных типа криптографии: симметричная и асимметричная. Симметричная криптография использует один и тот же ключ для шифрования и дешифрования данных, что может привести к утечке ключа, если он попадет в чужие руки. Асимметричная криптография, также известная как криптография с открытым ключом, использует два разных ключа - открытый и закрытый - для шифрования и дешифрования информации. Закрытый ключ хранится в тайне, а открытый может быть общедоступным.

Криптография также может быть классифицирована по уровню безопасности: низкая, средняя и высокая. Низкоуровневые методы шифрования, такие как XOR-шифр, могут быть легко взломаны, в то время как высокоуровневые алгоритмы, такие как RSA, считаются более надежными.

В данном разделе представлены классические и современные методы защиты информации.

Книжный шифр

Книжный шифрование – это метод шифрования, в котором каждая буква или слово в исходном тексте заменяется на ссылку (например, номер страницы, строки и столбца) соответствующего элемента в специальном тексте-ключе.

Для расшифровки необходимо иметь как зашифрованный текст, так и специальный ключ. В качестве дополнительного текста часто использовали распространенные литературные произведения, которые с большой долей вероятности были и у отправителя, и у адресата. Исключение: если в тексте-ключе отсутствует необходимая по смыслу буква (к примеру буква “Э”), то вместо неё используется буква «Е», но это никак не мешает расшифровке сообщения.

Пример шифрования:

Таблица 1. Пример шифрования. Книжный шифр

Исходное сообщение	Осень
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;
Зашифрованное сообщение	1/5, 4/2, 2/8, 3/3, 2/10.

Пояснение

Первая буква О - 1/5, где 1 - номер строки, 5 - номер столбца.

Таким образом, зашифрованное сообщение будет иметь следующий вид: 1/5, 4/2, 2/8, 3/3, 2/10.

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	1/5, 3/1, 4/16, 2/8, 2/3
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 2

Зашифрованное сообщение	4/2, 2/4, 1/1, 2/13, 1/15, 3/3, 4/8
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 3

Зашифрованное сообщение	2/8, 1/4, 2/1, 2/3, 3/5, 3/8, 3/3
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 4

Зашифрованное сообщение	2/1, 2/5, 3/9, 4/3, 2/17
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 5

Зашифрованное сообщение	4/2, 2/8, 4/2, 4/2, 4/14, 3/1, 2/6
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 6

Зашифрованное сообщение	1/4, 4/16, 3/1, 2/9, 2/4, 2/3
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 7

Зашифрованное сообщение	1,4/ 2/2, 3/11, 3/16
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 8

Зашифрованное сообщение	1/8, 2/3, 2/13, 4/14, 4/19
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 9

Зашифрованное сообщение	1/4, 1/16, 2/12, 4/1, 3/1, 3/3, 4/8, 3/15, 4/16, 3/5
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Вариант 10

Зашифрованное сообщение	3/1, 3/5, 4/13, 1/12, 2/1, 3/10, 4/2
Ключ	У лукоморья дуб зелёный; Златая цепь на дубе том: И днём и ночью кот учёный Всё ходит по цепи кругом;

Скитала

Скитала – это шифр, в котором ключом выступает предмет, обычно в виде шестигранной палочки.

На палочку наматывали кожаный ремень, а после писали сообщения по ребру. После того как ремень снимали, на нём оставался лишь набор символов.

Ключ для скиталы был закрытым — требовалось как минимум две одинаковые палочки: для автора сообщения и для читателя.

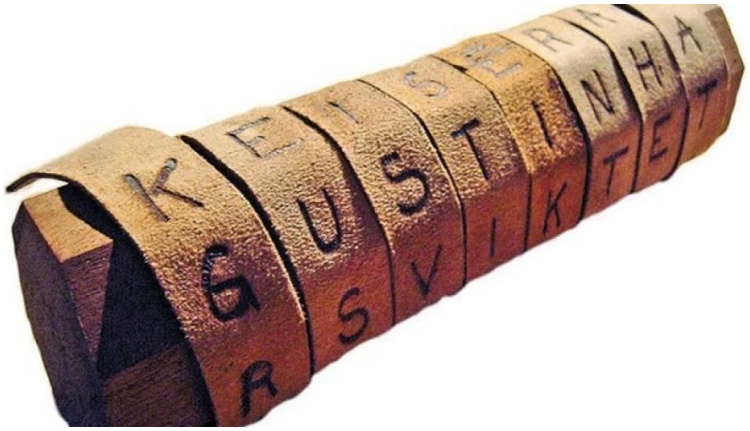

Рисунок 1. Жезл Скитала

Пример

Исходное сообщение РТУ_МИРЭА_ИИИ2023!

Пусть имеется палочка с тремя гранями(r=3), текст будет нанесен следующим образом:

Р	**Т**	**У**	**_**	**М**	**И**
Р	**Э**	**А**	**_**	**И**	**И**
И	**2**	**0**	**2**	**3**	**!**

Рисунок 2. Шифрование текста

Далее текст выписывается по столбцам снизу вверх слева направо.

Зашифрованное сообщения: ИРР2ЭТ0АУ2_ _ 3ИМ!ИИ.

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	Млмаиыш__иненахе_а
Ключ	r=3

Вариант 2

Зашифрованное сообщение	лдмуёуо_нбрлы_ьуйзяк.е_о
Ключ	r=4

Вариант 3

Зашифрованное сообщение	аемаЯн_аю_изш_деанде.деол
Ключ	r=5

Вариант 4

Зашифрованное сообщение	саДаюемттосикя_а_ктнаеат
Ключ	r=3

Вариант 5

Зашифрованное сообщение	рВсБя__е_толгудеомиелантуно_бекпо_иаммйр!о_у
Ключ	r=4

Вариант 6

Зашифрованное сообщение	лгО_онут_жопиврнии
Ключ	r=3

Вариант 7

Зашифрованное сообщение	ооюЯве__е_чпнмуоьгдменнн
Ключ	r=4

Вариант 8

Зашифрованное сообщение	юмаВчивсе,лян_е_ианже_ии_незре_ни_рьсии_кссуоуупвлар
Ключ	r=4

Вариант 9

Зашифрованное сообщение	_ебСтмиееьрмбяаье_ея_дт_Басноеяегт._ос_вмясы
Ключ	r=4

Вариант 10

Зашифрованное сообщение	н_зуначмсеуеоклчмжаьиунтзт-оьяьтс__сотвуя_ьоп
Ключ	r=5

Квадрат Полибия

Квадрат Полибия – это способ кодирования и шифрования текста, разработанный древнегреческим историком Полибием во 2 веке до н.э. Он представляет собой таблицу, в каждой ячейке которой записывается один символ текста. Затем каждая пара символов заменяется на определенный символ, который обозначает их позицию в таблице.

	1	**2**	**3**	**4**	**5**	**6**
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	_	,	.

Рисунок 3. Таблица шифрования для Квадрата Полибия

Для расшифровки текста необходимо знать размер таблицы и ключ замены символов. Этот метод шифрования был одним из первых, используемых для защиты конфиденциальной информации, и несмотря на свою простоту, он

обеспечивает некоторую степень защиты от несанкционированного доступа к тексту.

Пример

Слово для шифрования: МИРЭА

Метод 1

Для шифрования на квадрате находили букву текста и вставляли в шифровку нижнюю от неё в том же столбце. Если буква была в нижней строке, то брали верхнюю из того же столбца.

Буква текста:	М	И	Р	Э	А
Буква шифротекста :	Т	О	Ц	А	Ё

Рисунок 4. Пример шифрования первым методом

Метод 2

Сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально:

Буква:	М	И	Р	Э	А
Координата вертикальная:	2	4	6	1	1
Координата горизонтальная	3	2	3	6	1

Рисунок 5. Пример шифрования вторым методом

Затем координаты считывают по строкам:

24 61 13 23 61(*)

Далее координаты преобразуются в буквы по этому же квадрату:

Координата вертикальная:	2	6	1	2	6
Координата горизонтальная	4	1	3	3	1
Буква шифротекста :	Ю	Е	Л	М	Е

Рисунок 6. Пример шифрования вторым методом

Метод 3

Усложнённый вариант, который заключается в следующем: полученный первичный шифротекст (*) шифруется вторично. При этом он выписывается без разбиения на пары: 2461132361.

Полученная последовательность цифр сдвигается циклически влево на один шаг (нечётное количество шагов): 4611323612.

Эта последовательность вновь разбивается в группы по два: 46 11 32 36 12.

И по таблице заменяется на окончательный шифротекст:

Координата вертикальная:	4	1	3	3	1
Координата горизонтальная	6	1	2	6	2
Буква шифротекста :	_	А	З	Я	Ё

Рисунок 7. Пример шифрования третьим методом

Задача: Имея зашифрованное/исходное сообщение и ключ, получить исходное/зашифрованное сообщение.

Вариант 1

Расшифровать

Зашифрованное сообщение	БЧЪСЩАВЯЕЭГЛ
Ключ	2 метод

Вариант 2

Зашифровать

Исходное сообщение	ФИШИНГ
Ключ	3 метод

Вариант 3

Расшифровать

Зашифрованное сообщение	ЭКШ,ЦКГЦЁНЁГФШТКЦ.ГФЙОУГЦЁНГФШЦКМ.
Ключ	1 метод

Вариант 4

Зашифровать

Исходное сообщение	КРИПТОГРАФИЯ
Ключ	2 метод

Вариант 5

Расшифровать

Зашифрованное сообщение	ОЮРУГЯ
Ключ	3 метод

Вариант 6

Зашифровать

Исходное сообщение	БАНКНОТА
Ключ	3 метод

Вариант 7

Расшифровать

Зашифрованное сообщение	ЁЦЖЩН
Ключ	1 метод

Вариант 8

Расшифровать

Зашифрованное сообщение	Х,СКЧФЧ
Ключ	1 метод

Вариант 9

Зашифровать

Исходное сообщение	ПЫЛЕСОС
Ключ	2 метод

Вариант 10

Расшифровать

Зашифрованное сообщение	ГЯЦНУА
Ключ	3 метод

Магический квадрат

Магический квадрат – является шифром перестановки. Ключом является магический квадрат размером nxn. Магическим квадратом называется квадратная таблица, в которую занесены все числа от 1 до n^2 и обладающая тем свойством, что суммы элементов по столбцам совпадают с суммами элементов по строкам и совпадают с суммами элементов по главной и побочной диагоналями. Зашифрованное сообщение должно иметь длину n^2.

Буквы сообщения при шифровании нумеруются числами от 1 до n^2 и вписываются в магический квадрат в те ячейки, в которых стоит их номер. Для получения шифрограммы таблица читается по строкам.

Для расшифрования шифрограмма вписывается в магический квадрат по строкам, а читается в порядке следования чисел от 1 до n^2.

Таблица 2. Магический квадрат на 16 символов

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Пример

Исходное сообщение	УНИВЕРСИТЕТМИРЭА
Ключ	Магический квадрат таблица №
Зашифрованное сообщение	АИНИЕЕТИТРСМВЭРУ

Пояснение

Буквы сообщения при шифровании нумеруются числами от 1 до 16 и вписываются в магический квадрат в те ячейки, в которых стоит их номер

У	Н	И	В	Е	Р	С	И	Т	Е	Т	М	И	Р	Э	А
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Таблица 3. Зашифрованное сообщение

А	И	Н	И
Е	Е	Т	И
Т	Р	С	М
В	Э	Р	У

Для получения шифрограммы таблица читается по строкам.

Зашифрованное сообщение: АИНИЕЕТИТРСМВЭРУ

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	ьтввмириза тоотаа
Ключ	Магический квадрат табл. 2

Вариант 2

Зашифрованное сообщение	йрасоичафгретикк
Ключ	Магический квадрат табл. 2

Вариант 3

Зашифрованное сообщение	ькеттелыдовислет
Ключ	Магический квадрат табл. 2

Вариант 4

Зашифрованное сообщение	едаеодереоплиинр
Ключ	Магический квадрат табл. 2

Вариант 5

Зашифрованное сообщение	ллеопссфероиоанв
Ключ	Магический квадрат табл. 2

Вариант 6

Зашифрованное сообщение	еереяожовпрдминв
Ключ	Магический квадрат табл. 2

Вариант 7

Зашифрованное сообщение	ьурооемдъпонзтсг
Ключ	Магический квадрат табл. 2

Вариант 8

Зашифрованное сообщение	йувттелячысехинд
Ключ	Магический квадрат табл. 2

Вариант 9

Зашифрованное сообщение	ьидооенемврнntсе
Ключ	Магический квадрат табл. 2

Вариант 10

Зашифрованное сообщение	ьоеорёнеледнптсн
Ключ	Магический квадрат табл. 2

Шифр Цезаря

Шифр Цезаря – это вид шифра, в котором каждая буква заменяется на другую букву, которая находится на определенном расстоянии от нее в алфавите. Например, если используется смещение 1, то буква A будет заменяться на B, B на C и так далее. Если используется смещение 2, то A будет заменяться на C, B на D и так далее. Шифр назван в честь римского императора Цезаря, который использовал его для секретной переписки.

Таблица 4. Исходный алфавит

№	Буква	№	Буква	№	Буква
1	А	12	К	23	Х
2	Б	13	Л	24	Ц
3	В	14	М	25	Ч
4	Г	15	Н	26	Ш
5	Д	16	О	27	Щ
6	Е	17	П	28	Ъ
7	Ё	18	Р	29	Ы
8	Ж	19	С	30	Ь
9	З	20	Т	31	Э
10	И	21	У	32	Ю
11	Й	22	Ф	33	Я

Таблица 5. Пример шифрования

Исходное сообщение	МИРЭА
Ключ	k=3
Зашифрованное сообщение	ПЛФАГ

Задача: Имея зашифрованное сообщение и ключ, получить исходное сообщение.

Вариант 1

Зашифрованное сообщение	Чсмёифхмциц
Ключ, k	4

Вариант 2

Зашифрованное сообщение	Пнёйхтйчнпе
Ключ, k	5

Вариант 3

Зашифрованное сообщение	Мткcфретвцкб
Ключ, k	2

Вариант 4

Зашифрованное сообщение	Ылчусегрлз
Ключ, k	3

Вариант 5

Зашифрованное сообщение	Оуъфцтёьое
Ключ, k	6

Вариант 6

Зашифрованное сообщение	Шххзалфпл
Ключ, k	7

Вариант 7

Зашифрованное сообщение	Тцлршцйзхрм
Ключ, k	8

Вариант 8

Зашифрованное сообщение	Нултхсфлфхзпг
Ключ, k	3

Вариант 9

Зашифрованное сообщение	Ешчйтчнщнпеынд
Ключ, k	5

Вариант 10

Зашифрованное сообщение	Дпжтфмцр
Ключ, k	4

Атбаш

Шифр Атбаша – это древний шифр, который использовался для замены букв в тексте. В этом шифре каждая буква заменяется на букву, которая находится на том же месте в обратном порядке алфавита.

Таблица 6. Шифр Атбаш

Исходный алфавит

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Алфавит для шифрования

Я Ю Э Ь Ы Ъ Щ Ш Ч Ц Х Ф У Т С Р П О Н М Л К Й И З Ж Ё Е Д Г В Б А